

# -THURSDAY-

# DEF CON 25 SPEAKING SCHEDULE

## EVENING LOUNGES

Introducing DEF CON Evening Lounges

These are smaller more intimate talks that don't require audio and video support for a limited audience.

Panel - An Evening with the EFF

Friday at 20:00 - 22:00 in Trevi Room

Hacking Democracy, with Mr. Sean Kanuck

Friday at 20:00 - 22:00 in Capri Room

Horror stories of a translator and how a tweet can start a war with less than 140 characters, with El Kentaro

Friday at 20:00 - 22:00 in Modena

Panel - Meet the Feds (who care about security research)

Saturday at 20:00 - 22:00 in Capri Room

Panel - DO No H4RM: A Healthcare Security Conversation

Saturday at 20:00 - 22:00 in Modena Room

	101 Track 1	101 Track 2
10:00	There's no place like 127.0.0.1 - Achieving reliable DNS rebinding in modern browsers Luke Young	Where are the SDN Security Talks? Jon Medina
11:00	From Box to Backdoor: Using Old School Tools and Techniques to Discover Backdoors in Modern Devices Patrick DeSantis	Opt Out or Deauth Trying !- Anti-Tracking Bots Radios and Keystroke Injection Weston Hecker
12:00	Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode Matt Suiche	Jailbreaking Apple Watch Max Bazaliy
13:00	Amateur Digital Archeology Matt 'openfly' Joyce	Wiping Out CSRF Joe Rozner
14:00	Hacking the Cloud Gerald Steere & Sean Metcalf	See No Evil, Hear No Evil: Hacking Invisibly and Silently With Light and Sound Matt Wixe
15:00	Inside the "Meet Desai" Attack: Defending Distributed Targets from Distributed Attacks	Real-time RFID Cloning in the Field Dennis Maldonado
15:30	CINCVoFLT (Trey Forgety)	Exploiting Old Mag-stripe information with New technology Salvador Mendoza
16:00	DEF CON 101 Panel HighWiz, Malware Unicorn, Niki7a, Roamer, Wiseacre, & Shaggy	The Last CTF Talk You'll Ever Need: AMA with 20 years of DEF CON Capture-the-Flag organizers
17:00		Vulc@n, Hawaii John, Chris Eagle, Invisigoth, Caesar, & Myles

# -FRIDAY-

	DEF CON 101	Track 2	Track 3	Track 4
10:00	<p>macOS/iOS Kernel Debugging and Heap Feng Shui</p> <p>Min(Spark) Zheng &amp; Xiangyu Liu</p>	<p>Welcome to DEF CON 25</p> <p>The Dark Tangent</p>	<p>The Brain's Last Stand</p> <p>Garry Kasparov</p>	<p>Secret Tools: Learning About Government Surveillance Software You Can't Ever See</p> <p>Peyton "Foofus" Engel</p>
10:30	<p>Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&amp;C Server</p> <p>Patrick Wardle</p>	<p>Hacking travel routers like it's 1999</p> <p>Mikhail Sosonkin</p>		<p>Panel: Meet The Feds</p> <p>Andrea Matwyshyn, Terrell McSweeney, Dr. Suzanne Schwartz, &amp; Leonard Bailey</p>
11:00	<p>Rage Against the Weaponized AI Propaganda Machine</p> <p>Suggy (AKA Chris Sumner)</p>	<p>Weaponizing the BBC Micro:Bit</p> <p>Damien "virtualabs" Cauquil</p>	<p>Hacking Smart Contracts</p> <p>Konstantinos Karagiannis</p>	
12:00	<p>CITL and the Digital Standard - A Year Later</p> <p>Sarah Zatko</p>	<p>Open Source Safe Cracking Robots - Combinations Under 1 Hour! (Is it bait? Damn straight it is.)</p> <p>Nathan Seidle</p>	<p>A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages!</p> <p>Orange Tsai</p>	<p>Hacking Democracy: A Socratic Dialogue</p> <p>Mr. Sean Kanuck</p>
13:00	<p>Controlling IoT Devices With Crafted Radio Signals</p> <p>Caleb Madrigal</p>	<p>Teaching Old Shellcode New Tricks</p> <p>Josh Pitts</p>	<p>Starting the Avalanche: Application DoS In Microservice Architectures</p> <p>Scott Behrens &amp; Jeremy Heffner</p>	<p>Next-Generation Tor Onion Services</p> <p>Roger Dingledine</p>
14:00	<p>Using GPS Spoofing to Control Time</p> <p>David "Karit" Robinson</p>	<p>Death By 1000 Installers; on MacOS, It's All Broken!</p> <p>Patrick Wardle</p>	<p>Breaking the x86 Instruction Set</p> <p>Christopher Domas</p>	<p>How We Created the First SHA-1 Collision and What it means For Hash Security</p> <p>Elie Bursztein</p>
15:00	<p>Assembly Language is Too High Level</p> <p>XlogicX</p>	<p>Phone System Testing and Other Fun Tricks</p> <p>"Snide" Owen</p>	<p>Dark Data</p> <p>Svea Eckert &amp; Andreas Dewes</p>	<p>Abusing Certificate Transparency Logs</p> <p>Hanno Böck</p>
16:00	<p>Radio Exploitation 101: Characterizing, Contextualizing, and Applying Wireless Attack Methods</p> <p>Matt Knight &amp; Marc Newlin</p>	<p>The Adventures of AV and the Leaky Sandbox</p> <p>Itzik Kotler &amp; Amit Klein</p>	<p>An ACE Up the Sleeve: Designing Active Directory DACL Backdoors</p> <p>Andy Robbins &amp; Will Schroeder</p>	<p>"Tick, Tick, Tick. Boom! You're Dead." - Tech &amp; the FTC</p> <p>Whitney Merrill &amp; Terrell McSweeney</p>
17:00	<p>Cisco Catalyst Exploitation</p> <p>Artem Kondratenko</p>	<p>Panel - DEF CON Groups</p>	<p>MEATPISTOL, A Modular Malware Implant Framework</p> <p>FuzzyNop (Josh Schwartz) &amp; ceyx (John Cramb)</p>	<p>The Internet Already Knows I'm Pregnant</p> <p>Cooper Quintin &amp; Kashmir Hill</p>

# -SATURDAY-

	DEF CON 101	Track 2	Track 3	Track 4
10:00	<p>Persisting with Microsoft Office: Abusing Extensibility Options</p> <p>William Knowles</p>	<p>\$BIGNUM Steps Forward, \$TRUMPNUM Steps Back: How Can We Tell If We're Winning?</p> <p>Cory Doctorow</p>	<p>Get-\$pwnd: Attacking Battle-Hardened Windows Server</p> <p>Lee Holmes</p>	<p>The spear to break the security wall of S7CommPlus</p> <p>Cheng</p>
10:30	<p>Breaking Wind: Adventures in Hacking Wind Farm Control Networks</p> <p>Jason Staggs</p>		<p>WSUSpendu: How to Hang WSUS Clients</p> <p>Romain Coltel &amp; Yves Le Provost</p>	<p>(Un)Fucking Forensics: Active/Passive (i.e. Offensive/Defensive) Memory Hacking/Debugging.</p> <p>K2</p>
11:00	<p>Microservices and FaaS for Offensive Security</p> <p>Ryan Baxendale</p>	<p>Secure Tokin' and Doobiekeys: How to Roll Your Own Counterfeit Hardware Security Devices</p> <p>Joe FitzPatrick &amp; Michael Leibowitz</p>	<p>If You Give a Mouse a Microchip... It Will Execute a Payload and Cheat At Your High-stakes Video Game Tournament</p>	<p>Evading Next-Gen AV Using Artificial Intelligence</p> <p>Hyrum Anderson</p>
11:30	<p>Abusing Webhooks for Command and Control</p> <p>Dimitry Snezhkov</p>		<p>skud (Mark Williams) &amp; Sky (Rob Stanley)</p>	<p>All Your Things Are Belong To Us</p>
12:00	<p>Driving down the rabbit hole</p> <p>Mickey Shkatov, Jesse Michael, &amp; Oleksandr Bazhaniuk</p>	<p>When Privacy Goes Poof! Why It's Gone and Never Coming Back</p> <p>Richard Thieme a.k.a. neuralcowboy</p>	<p>DNS - Devious Name Services - Destroying Privacy &amp; Anonymity Without Your Consent</p> <p>Jim Nitterauer</p>	<p>Zenofex, 0x00string, CJ_000, &amp; Maximus64</p>
13:00	<p>Demystifying Windows Kernel Exploitation by Abusing GDI Objects.</p> <p>5A1F (Saif El-Sherai)</p>	<p>Koadic C3 - Windows COM Command &amp; Control Framework</p> <p>Sean Dillon (zerosum0x0) &amp; Zach Harding (Aleph-Naught-)</p>	<p>Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits</p> <p>Manfred (@_EBFE)</p>	<p>A Picture is Worth a Thousand Words, Literally: Deep Neural Networks for Social Stego</p> <p>Philip Tully &amp; Michael T. Raggo</p>
14:00	<p>Attacking Autonomic Networks</p> <p>Omar Eissa</p>	<p>Trojan-tolerant Hardware &amp; Supply Chain Security in Practice</p> <p>Vasilios Mavroudis &amp; Dan Cvrcek</p>	<p>Linux-Stack Based V2X Framework: All You Need to Hack Connected Vehicles</p> <p>p3n3troot0r (Duncan Woodbury) &amp; ginsback (Nicholas Haltmeyer)</p>	<p>XenoScan: Scanning Memory Like a Boss</p> <p>Nick Cano</p>
15:00	<p>MS Just Gave the Blue Team Tactical Nukes (And How Red Teams Need To Adapt)</p> <p>Chris Thompson</p>	<p>Tracking Spies in the Skies</p> <p>Jason Hernandez, Sam Richards, &amp; Jerod MacDonald-Evoy</p>	<p>DOOMed Point of Sale Systems</p> <p>trixr4skids</p>	<p>Digital Vengeance: Exploiting the Most Notorious C&amp;C Toolkits</p> <p>Professor Plum</p>
16:00	<p>Dealing the Perfect Hand - Shuffling Memory Blocks On z/OS</p> <p>Ayoul3</p>	<p>From "One Country - One Floppy" to "Startup Nation" - The Story of the Early Days of the Israeli Hacking Community, and the Journey Towards Today's Vibrant Startup Scene</p> <p>Inbar Raz &amp; Eden Shochat</p>	<p>CableTap: Wirelessly Tapping Your Home Network</p> <p>Marc Newlin, Logan Lamb, &amp; Chris Grayson</p>	<p>Game of Drones: Putting the Emerging "Drone Defense" Market to the Test</p> <p>Francis Brown &amp; David Latimer</p>
17:00	<p>Here to stay: Gaining persistency by Abusing Advanced Authentication Mechanisms</p> <p>Marina Simakov &amp; Igal Gofman</p>		<p>Taking Windows 10 Kernel Exploitation to the next level - Leveraging write-what-where vulnerabilities in Creators Update</p> <p>Morten Schenk</p>	<p>Introducing HUNT: Data Driven Web Hacking &amp; Manual Testing</p> <p>Jason Haddix</p>

# -SUNDAY-

	DEF CON 101	Track 2	Track 3	Track 4
10:00	<p><b>Unboxing Android: Everything You Wanted To Know About Android Packers</b></p> <p>Avi Bashan &amp; Slava Makkaveev</p>	<p><b>I Know What You Are by the Smell of Your Wifi</b></p> <p>Denton Gentry</p>	<p><b>Breaking Bitcoin Hardware Wallets</b></p> <p>Josh Datko &amp; Chris Quartier</p>	<p><b>Untrustworthy Hardware and How to Fix It</b></p> <p>Øctane</p>
10:30		<p><b>PEIMA (Probability Engine to Identify Malicious Activity): Using Power Laws to address Denial of Service Attacks</b></p> <p>Redezem</p>	<p><b>BITSinject</b></p> <p>Dor Azouri</p>	<p><b>Ghost in the Droid: Possessing Android Applications with ParaSpectre</b></p> <p>chaosdata</p>
11:00	<p><b>Total Recall: Implanting Passwords in Cognitive Memory</b></p> <p>Tess Schrodinger</p>	<p><b>Backdooring the Lottery and Other Security Tales in Gaming over the Past 25 Years</b></p> <p>Gus Fritschie &amp; Evan Teitelman</p>	<p><b>Exploiting Continuous Integration (CI) and Automated Build systems</b></p> <p>spaceB0x</p>	<p><b>Ghost Telephonist' Impersonates You Through LTE CSFB</b></p> <p>Yuwei Zheng &amp; Lin Huang</p>
12:00	<p><b>The Black Art of Wireless Post Exploitation</b></p> <p>Gabriel "solstice" Ryan</p>	<p><b>Are all BSDs are created equally? A survey of BSD kernel vulnerabilities.</b></p> <p>Ilja van Sprundel</p>	<p><b>The Call Is Coming From Inside the House! Are You Ready for the Next Evolution in DDoS Attacks?</b></p> <p>Steinthor Bjarnason &amp; Jason Jones</p>	<p><b>Genetic Diseases to Guide Digital Hacks of the Human Genome: How the Cancer Moonshot Program will Enable Almost Anyone to Crash the Operating System that Runs You or to End Civilization...</b></p> <p>John Sotos</p>
13:00	<p><b>Game of Chromes: Owning the Web with Zombie Chrome Extensions</b></p> <p>Tomer Cohen</p>	<p><b>Bypassing Android Password Manager Apps Without Root</b></p> <p>Stephan Huber &amp; Siegfried Rasthofer</p>	<p><b>Malicious CDNs: Identifying Zbot Domains en Masse via SSL Certificates and Bipartite Graphs</b></p> <p>Thomas Mathew &amp; Dhia Mahjoub</p>	<p><b>Revoke-Obfuscation: PowerShell Obfuscation Detection (And Evasion) Using Science</b></p> <p>Daniel Bohannon (DBO) &amp; Lee Holmes</p>
14:00	<p><b>Call the Plumber - You Have a Leak in Your (Named) Pipe</b></p> <p>Gil Cohen</p>	<p><b>Weaponizing Machine Learning: Humanity Was Overrated Anyway</b></p> <p>Dan "AltF4" Petro &amp; Ben Morris</p>	<p><b>Man in the NFC</b></p> <p>Haoqi Shan &amp; Jian Yuan</p>	<p><b>Friday the 13th: JSON attacks!</b></p> <p>Alvaro Muñoz &amp; Oleksandr Mirosh</p>
15:00		<p><b>25 Years of Program Analysis</b></p> <p>Zardus (Yan Shoshitaishvili)</p>		
16:30			<p><b>Closing Ceremonies</b></p>	
17:00				